REMARKS

Claims 1-18 are pending in the present application.

Claim Rejections - 35 U.S.C. §103

Claims 1-5 and 13-18 were rejected under 35 U.S.C. §103(a) as being unpatentable over ***Hasebe*** (U.S. Patent No. 5,392,351) in view of ***Lang*** (U.S. Patent No. 5,191,611); and claims 6-12 were rejected under 35 U.S.C. §103(a) as being unpatentable over *Hasebe* in view of *Lang* as applied to claims 1-5 above, and further in view of ***Shear*** (U.S. Patent Application Publication No. 2001/042043). Favorable reconsideration of the rejection is requested.

A. User Information Hold Unit

In the previous arguments, (Amendment, filed September 15, 2005, pages 11-14), Applicants stated that *Hasebe* does not disclose a user information hold unit for identifying a user of a recording device as recited in claim 1. In response, the Examiner stated that the personal key generating unit of *Hasebe* is a user information hold unit, and that the personal key generating unit generates a user's personal key using the user's personal number. (Office Action, page 2.)

Applicants respectfully submit that the personal number is not information identifying a user, thus the personal key generating unit of *Hasebe* is not an information hold unit for identifying a user of a recording device as recited in claim 1.

The personal number is only used for generating a personal key in the vendor computer and the user's computer. The personal key is used for encrypting the software decryption key on

the vendor computer and for decrypting the software decryption key in the user computer. (Col. 3, lines 40-50.)

The personal number is not user information for identifying a user. The personal number is "for example, an apparatus number of a computer." (Col. 3, lines 40-43.) *Hasebe* discloses that a personal number is a number that is unique to a computer, meaning that a user cannot decrypt the software from a different computer. In other words, the personal number does not identify a user. *Hasebe* states:

> In use of the **personal number for the computer**, the execution for the computer is applied by the permission information 72 so that **only that computer can execute** the plain text software. Accordingly, the user cannot utilize a different computer even if he is authorized. Further, it is impossible to transfer such plain text software to a third-party.

(Col. 3, lines 60-66, emphasis added.)

Furthermore, even if the personal number does identify a user, as alleged by the Examiner, *Hasebe* does not disclose "a user information hold unit *for holding first user ID data*" as recited in claim 1. The personal key generating unit does not "hold" the personal number. The personal key generating unit processes the personal number into a personal key. Nothing in the personal key generating unit can be used to identify a user. The personal key generating unit does not hold information at all.

Hasebe does not disclose "first user ID data provided to identify a user of said recording device" nor does *Hasebe* disclose "a user information hold unit for holding" such data.

Therefore, the combination of *Hasebe* and *Lang* does not disclose the elements as recited in claim 1.

B. Control Unit

The previous arguments also stated that *Hasebe* does not disclose a control unit controlling operation of the recording device by referring to protection information to restrict access to the encrypted data as recited in claim 1. In response, the Examiner stated that the decrypting circuit 93 of *Hasebe* is a control unit, and that the decrypting circuit decrypts the permission information 72 from the software storage medium 71 based on the personal key 81.

Applicants respectfully submit that the decrypting circuit 93 of *Hasebe* does not control the operation of the recording device, thus *Hasebe* does not disclose:

> a control unit controlling the operation of said recording device, said control unit referring to said protection information to restrict external access to said encrypted content data held in said first storage unit

as recited in claim 1.

In the present invention, protection information, such as a reproduction flag, is referred to before proceeding to decryption of the encrypted data. For example, if the content reproduction flag is set in a status allowing content data to be reproduced then controller 1420 allows the decryption unit 1416 to decrypt encrypted data. (Specification, page 21, lines 2-15; Fig. 11.) Otherwise, if the content reproduction flag is set in a status such that content data is not to be reproduced, then controller 1420 proceeds on a different processing path and may disallow reproduction of the content data. (Specification, page 21, lines 16-31; Fig. 11.)

The decrypting circuit 93 of *Hasebe* decrypts permission information 72 using the personal key generated by the personal key generating unit. The decrypting circuit does not refer to protection information to restrict access to the encrypted permission information. The decrypting circuit does not have any logic for determining whether certain conditions are met before decryption proceeds. The decryption circuit blindly attempts decryption. If the personal key is incorrect then the decryption attempted by the decryption circuit fails. The decryption circuit does not refer to protection information before attempting to decrypt the data.

Hasebe does not disclose a control unit controlling the operation of the recording device or a control unit that refers to protection information to restrict external access to encrypted content data. Therefore, the combination of *Hasebe* and *Lang* does not disclose the elements as recited in claim 1.

C. Protection Information Memory Unit

In the previous arguments, Applicants argued that *Lang* does not disclose a protection information memory unit which is updatable in response to a result of comparing externally provided user information with said first user ID data, as externally instructed. The Examiner did not respond to this argument.

Applicants respectfully submit that neither *Hasebe* nor *Lang* disclose:

> a protection information memory unit holding protection information updatable in response to a result of comparing externally provided user information with said first user ID data, as externally instructed

as recited in claim 1.

Protection information, as defined in the specification of the present invention, is information such as whether or not additional recording is allowed on the recording device and whether or not data is erasable on the recording device. (Specification, page 8.) Protection information is set by the user.

The Examiner cites permission information 13 of *Hasebe* as being the protection information as recited in claim 1. Permission information 13 is encrypted data for decrypting the encrypted software. Permission information is an encrypted software decryption key and is generated by the vendor computer by encrypting the software decrypting key. (*Hasebe*, Col. 5, lines 40-45; Figs. 1-3.) *Hasebe* does not disclose protection information such as whether or not additional recording is allowed and whether or not data is erasable.

Furthermore, even if *Hasebe* discloses a protection information memory unit holding protection information, neither *Hasebe* nor *Lang* disclose that the protection information is updatable in response to a result of comparing externally provided user information with the first user ID data, as externally provided.

The Examiner acknowledges that *Hasebe* does not disclose that protection information is updatable in response to a result of comparing externally provided user information with said first user ID data. The Examiner cites *Lang* at col. 12, lines 36-58 for disclosing such a feature. This passage states a procedure for limiting and controlling user privileges to information. The procedure first states that authorized users are given a specific number of information retrievals. Once the specific number of retrievals has been reached, the user must renew or update privileges

to information. To renew user privileges, the user must request renewal. Then the **user is given** an updated access code.

In the present invention, protection information is updated **by the user**. (Specification, page 19, lines 13-31; Fig. 10.) Once the recording device determines that the externally provided user information matches the first user ID stored in the recording device, the user is allowed to update the information. In *Lang*, information is protected by restricting access to users. Whereas in the present invention, the user controls the protection of information on the recording device.

Neither *Hasebe* nor *Lang* disclose a protection information memory unit holding protection information updatable in response to a result of comparing externally provided user information with the first user ID data, as externally provided. Therefore, the combination of *Hasebe* and *Lang* does not disclose all of the elements as recited in claim 1.

D. Recording Device Detachably Attachable to a Reproduction Apparatus

Applicants respectfully submit that neither *Hasebe* nor *Lang* disclose "a recording device detachably attachable to a reproduction apparatus" as recited in claim 1.

The present invention relates to a memory card that is accommodated by a recording device. The memory card has a data input/output unit, a first storage unit, a user information hold unit, a protection information memory unit, and a control unit.

Neither *Hasebe* nor *Lang* disclose a circuit having the above elements in the storage media. Therefore, neither *Hasebe* nor *Lang* disclose the elements as recited in claim 1.

Accordingly, withdrawal of the rejection of claims 1-18 is hereby solicited.

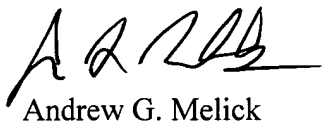
In view of the above-mentioned remarks, Applicants submit that that the claims are in condition for allowance. Applicants request such action at an early date.

If the Examiner believes that this application is not now in condition for allowance, the Examiner is requested to contact Applicants' undersigned attorney to arrange for an interview to expedite the disposition of this case.

If this paper is not timely filed, Applicants respectfully petition for an appropriate extension of time. The fees for such an extension or any other fees that may be due with respect to this paper may be charged to Deposit Account No. 50-2866.

Respectfully submitted,

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP



Andrew G. Melick
Attorney for Applicants
Registration No. 56,868
Telephone: (202) 822-1100
Facsimile: (202) 822-1111

AGM/sg